IOPscience iopscience.iop.org

Home Search Collections Journals About Contact us My IOPscience

Focus on device independent quantum information

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2016 New J. Phys. 18 100202

(http://iopscience.iop.org/1367-2630/18/10/100202)

View the table of contents for this issue, or go to the journal homepage for more

Download details:

IP Address: 131.215.70.231
This content was downloaded on 02/12/2016 at 15:55

Please note that terms and conditions apply.

You may also be interested in:

Device-independent quantum key distribution secure against collective attacks
Stefano Pironio, Antonio Acín, Nicolas Brunner et al.

Private randomness expansion with untrusted devices
Roger Colbeck and Adrian Kent

Security of a practical semi-device-independent quantum key distribution protocol against collective attacks
Wang Yang, Bao Wan-Su, Li Hong-Wei et al.

Optimal randomness generation from optical Bell experiments
Alejandro Máttar, Paul Skrzypczyk, Jonatan Bohr Brask et al.

Quantum randomness extraction for various levels of characterization of the devices
Yun Zhi Law, Le Phuc Thinh, Jean-Daniel Bancal et al.

Device-independent bit commitment based on the CHSH inequality
N Aharon, S Massar, S Pironio et al.

Measurement-device–independent randomness from local entangled states
Anubhav Chaturvedi and Manik Banik

Implementations for device-independent quantum key distribution
Alejandro Máttar and Antonio Acín

Bipartite Bell inequalities with three ternary-outcome measurements—from theory to experiments
Sacha Schwarz, Bänz Bessire, André Stefanov et al.

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

PUBLISHED
31 October 2016

Original content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence.

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

EDITORIAL

Focus on device independent quantum information

S Pironio[1], V Scarani[2] and T Vidick[3]

[1] Laboratoire d'Information Quantique, CP 224, Universite libre de Bruxelles (ULB), 1050 Bruxelles, Belgium
[2] Centre for Quantum Technologies and Department of Physic, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore
[3] Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, USA

The field of quantum information is born out of a sequence of surprising discoveries in the 1980s, all building on the same deep insight: the counter-intuitive quantum properties of particles such as photons or electrons can be put to task in order to accomplish certain computational, cryptographic, and information-theoretic tasks impossible to realize by purely classical means. A famous example is the cryptographic problem of key distribution, for which Bennett and Brassard devised the first quantum protocol in 1984 [6] and whose security relies on the no-cloning principle of quantum mechanics. Another example is the computational problem of factoring large numbers, for which Shor devised the first efficient quantum algorithm in 1994 [32] by exploiting the possibility for quantum systems to evolve in superpositions of exponentially many different states.

In this early history, and until very recently, the violation of Bell inequalities was simply seen as yet another feature distinguishing the quantum processing of information from a classical one. It provided one of the initial motivations for developing a better understanding of entangled states; it was recognized as a key factor responsible for the quantum advantage in communication complexity protocols; it was frequently used in experiments to demonstrate one's ability to generate and manipulate entanglement. It also played an important conceptual role, as it established that the predictions of quantum theory, including its claimed information processing advantages, could not be naively reproduced by a classical theory. But overall the manifestation of quantum non-locality was just another way to evidence the weirdness of quantum theory, on par with the no-cloning principle or the uncertainty of quantum measurements in having little consequence for practical applications.

In very recent years, however, the violation of Bell inequalities has acquired a special status that is starting to revolutionize our understanding of the information-theoretic possibilities of quantum information. Indeed, not only are the properties of quantum states and measurements leading to the violation of Bell inequalities unique in the sense of having no classical explanation, but they also often uniquely single out the quantum system itself. More precisely, given a black-box device that is verifiably violating a Bell inequality, quantum theory allows for a virtually unique way in which this can be accomplished. Furthermore, for the many tasks for which quantum information provides an advantage, there often turns out to be a protocol whose advantage essentially amounts to the sufficiently large violation of a certain Bell inequality.

Taken together, these two phenomena lead to the following observation: it is possible to devise quantum information protocols whose correctness can be certified even when they are run with untrusted quantum devices, on which no *a priori* assumptions are made. Hence the name 'device-independence' (DI) to refer to such protocols. The implications of this are profound; many are discussed in this issue. Most notably, it allows for certifiable cryptographic randomness generation (RNG) and key distribution (QKD) with unprecedented security.

This intuition for device independence was already at the origin of Ekert's quantum key distribution proposal in 1991 [11]. But the first security proof of QKD explicitly based on the violation of a Bell inequality had to wait till 2007, in the very same paper in which the wording 'device-independent' (DI) was introduced [1]. This re-discovery came after a tortuous path that we won't review in detail. Let us stress a few precursors. From the side of cryptography, the clear precursor is work of Mayers and Yao, who had the idea of DIQKD back in 1998 [17]. Mayers and Yao couldn't provide a security proof, but they demonstrated the possibility of 'self-testing': some observable statistics identify uniquely a state and the corresponding measurements. (Unbeknownst to them, a similar result had been noticed in the field of nonlocality for the maximal violation of the Clauser-Horne-Shimony-Holt inequality, but without any suggestion that this could have applied value [26, 33].) From the side of nonlocality, the work of Popescu and Rohrlich on no-signaling boxes [27] led Barrett, Hardy and Kent

© 2016 IOP Publishing Ltd and Deutsche Physikalische Gesellschaft

to intuit that the security of key distribution could be proved without providing a quantum description of the apparatuses used: it is enough that they do not allow arbitrary transmission of signals [4]. Later on, Colbeck and Kent asked if similar ideas could be used for the related problem of cryptographic randomness expansion [9, 10], leading Pironio *et al* to introduce in 2010 the first protocol, security proof and experimental demonstration for this task [22].

After the 2007 paper on DIQKD and 2010 paper on DIRNG, the field of DI certification of quantum devices blossomed. Initially, one of the biggest challenges on the theoretical side had been focused on demonstrating that secure fully DI RNG and QKD are possible in principle. The security of DI QKD and RNG was first established under restricting assumptions on the devices [1, 13, 15, 16] or the adversary [21–23]. Only very recently it has finally been established in the most general setting [19, 29, 38]. Though developing better security proofs remains an important goal (see recent work by Arnon-Friedman *et al* [3]), now that we know that full DI security is possible in principle, part of the research interest has shifted towards other directions. This 'focus on' collection aims at bringing together these new and recent efforts.

- A first area of focus is to closing the gap between theory and experiments. Present security analyses make very demanding experimental requirements, such as the necessity to manipulate entangled states with high efficiency and fidelity; little noise is tolerated on the communication channels. Moreover, they tend to be applied to ad-hoc protocols that do not take into account the specificity of particular implementations, such as the (by far) sub-unity detection efficiency of photonic systems, in a satisfactory way.
  A promising path to the design of more experimentally friendly protocols is to make stronger assumptions on the devices, keeping the spirit of device independence while acknowledging differences in the level of trust about the quantum devices used that can be justified in the context of a realistic implementations.
  Among the results presented in this issue, [35] study a 'semi-device-independent' (SDI) model in which one of the devices is trusted; in this scenario they provide improved quantitative bounds for the problem of self-testing an EPR pair, with an analysis based on the phenomenon of EPR steering. [12] considers another SDI model, one in which only the dimension of the system is known but not the measurements, and provides tools to quantify entanglement and security proofs for QKD. [40] studies the security of BB84 under the even weaker assumption that the dimension of only one of the systems is constrained to be a qubit. [20] shows that considering higher-dimensional systems (still in the SDI model, where a bound on the dimension of the devices is given *a priori*) can lead to improve rates, albeit at a higher computational cost. [7] consider the task of RNG in the 'measurement-device independent' MDI) setting, where the source, but not the detector, are trusted; their analysis allows them to handle high losses at the untrusted detector and leads to a more practical protocol which (in contrast to fully DI protocols) does not require the generation of entangled states. In the fully device-independent setting (but under an i.i.d. assumption), [37] provide theoretical justification for the use of the fair sampling assumption in accounting for non-detection events.
- Practical implementations also reveal the limits of the device-independent model: as any model for security, device-independence makes a set of assumptions, such as perfect isolation of the trusted users' laboratories, that may in practice be (at least partially) compromised. How robust is the model? The authors of [36] consider precisely this issue, and explore the possibility of allowing for a small amount of information leakage about basis choices, in a specific optical setup. A different assumption is the use of perfect trusted random number generators by the honest users. The paper [28] relaxes such 'free will' assumption and investigates Bell inequalities in the presence of small amounts of measurement dependence. Other variations on the standard model for device independence are possible, and may lead to protocols with theoretical or practical advantages. [5] considers the class of correlations that can be said to derive from causal order. [25] analyses experimental data using inequalities based on Kolmogorov complexity instead of the standard local causality condition.
- Beyond key distribution, it is interesting to investigate if the device-independent approach to security can be extended to other tasks in multi-party cryptography. A prominent target are tasks in two-party cryptography, such as bit commitment, which is investigated in [2]. In [14] the authors use results in the noisy-storage model as starting point and give a device-independent protocol for a universal primitive in that model, weak string erasure.
  Aside from its application to cryptography, the idea of self-testing is further developing as an independent field, integrating the approach of Mayers-Yao with that based on Bell inequalities. A zoology of states and measurements have been proved to be identifiable in this way, and robust bounds were obtained that tolerate imperfections in the observed statistics. Two examples from this issue are [39], where all possible self-tests for

the singlet are characterized, and [18] that investigates the use of an elementary Bell inequality 'in parallel', allowing to simultaneously self-test multiple copies of a basic state.

- The area of device independent cryptography is born out of an interest in coming to grips with the nonlocal aspects of quantum mechanics, as evidenced by Bell inequalities. It is fitting that progress in the area ultimately rests on a deeper understanding of the relative strengths and merits of different classes of inequalities. This issue contains a number of results in this direction, painting a diverse picture of the 'nonlocality landscape', now often reformulated as *multiplayer games*. The authors of [30] study linear games, a generalization of XOR games, which correspond to correlation inequalities. [24] study a different variation of XOR games, so-called CHSH_q games. [8] construct games based on random access codes, [34] investigate the advantages of using Chained Bell inequalities for randomness generation, and [31] explore Bell inequalities with ternary outcomes.

From its origins in the study of 'quantum spookyness' and the early discovery of its potential for cryptography, the study of the consequences of quantum non-locality for information processing tasks has blossomed into a increasingly diverse field, which provides a powerful vantage point for tackling some of the most important challenges of quantum information theory. A prominent example are the related tasks of delegating quantum computations, and testing quantum systems: as the size, and complexity, of practical systems scales well beyond what can be characterized via complete tomographic methods, the only control on quantum devices will become, by force, of device-independent nature.

Rising to this challenge will require overcoming many barriers, some technical and some conceptual. Robustness bounds, especially for the parallel or sequential self-testing of many-qubit states, need to be improved; the classes of states for which self-tests are known needs to be expanded. Experimental challenges abound as well, as basic applications such as randomness amplification still require states and operations that are far from feasible in the state-of-the-art. We are confident that the works reported in this Focus will prove important milestones in these future developments.

References

[1] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 Device-independent security of quantum key distribution against collective attacks *Phys. Rev. Lett.* **98** 230501
[2] Aharon N, Massar S, Pironio S and Silman J 2016 Device-independent bit commitment based on the chsh inequality *New J. Phys.* **18** 025014
[3] Arnon-Friedman R, Renner R and Vidick T 2016 arXiv:1607.01797
[4] Barrett J, Hardy L and Kent A 2005 No signaling and quantum key distribution *Phys. Rev. Lett.* **95** 010503
[5] Baumeler A and Wolf S 2016 Device-independent test of causal order and relations to fixed-points *New J. Phys.* **18** 035014
[6] Bennett C and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE ICCSSP* **560** 175–9
[7] Cao Z, Zhou H and Ma X 2015 Loss-tolerant measurement-device-independent quantum random number generation *New J. Phys.* **17** 125011
[8] Chailloux A, Kerenidis I, Kundu S and Sikora J 2016 Optimal bounds for parity-oblivious random access codes *New J. Phys.* **18** 045003
[9] Colbeck R 2006 Quantum and relativistic protocols for secure multi-party computation *PhD Thesis* Trinity College, University of Cambridge
[10] Colbeck R and Kent A 2011 Private randomness expansion with untrusted devices *J. Phys. A: Math. Theor.* **44** 095305
[11] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3
[12] Goh K T, Bancal J-D and Scarani V 2016 Measurement-device-independent quantification of entanglement for given hilbert space dimension *New J. Phys.* **18** 045022
[13] Hänggi E, Renner R and Wolf S 2010 Efficient device-independent quantum key distribution *Proc. 29th EUROCRYPT* (Berlin: Springer) pp 216–34
[14] Kaniewski J and Wehner S 2016 Device-independent two-party cryptography secure against sequential attacks *New J. Phys.* **18** 055004
[15] Masanes L, Pironio S and Acn A 2011 Secure device-independent quantum key distribution with causally independent measurement devices *Nat. Commun.* **2** 7
[16] Masanes L, Renner R, Christandl M, Winter A and Barrett J 2009 Unconditional security of key distribution from causality constraints Technical report arXiv:quant-ph/0606049v4
[17] Mayers D and Yao A 1998 Quantum cryptography with imperfect apparatus *Proc. 39th FOCS* (Washington, DC: IEEE Computer Society) p 503
[18] McKague M 2016 Self-testing in parallel *New J. Phys.* **18** 045013
[19] Miller C A and Shi Y 2014 Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices *Proc. 46th STOC* (New York: ACM)
[20] Mironowicz P, Tavakoli A, Hameedi A, Marques B, Pawłowski M and Bourennane M 2016 Increased certification of semi-device independent random numbers using many inputs and more post-processing *New J. Phys.* **18** 065004
[21] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 Device-independent quantum key distribution secure against collective attacks *New J. Phys.* **11** 045021
[22] Pironio S, Acín A, Massar S, De La Giroday A B, Matsukevich D N, Maunz P, Olmschenk S, Hayes D, Luo L and Manning T A 2010 Random numbers certified by Bell's theorem *Nature* **464** 10
[23] Pironio S, Masanes L, Leverrier A and Acín A 2013 Security of device-independent quantum key distribution in the bounded-quantum-storage model *Phys. Rev.* X **3** 031007
[24] Pivoluska M and Plesch M 2016 An explicit classical strategy for winning a chsh_q game *New J. Phys.* **18** 025013

[25] Poh H S, Markiewicz M, Kurzyński P, Cerè A, Kaszlikowski D and Kurtsiefer C 2016 Probing the quantum/classical boundary with compression software *New J. Phys.* **18** 035011
[26] Popescu S and Rohrlich D 1992 Which states violate the bell inequality maximally? *Phys. Lett.* A **169** 411
[27] Popescu S and Rohrlich D 1994 Quantum nonlocality as an axiom *Found. Phys.* **24** 379–85
[28] Putz G and Gisin N 2016 Measurement dependent locality *New J. Phys.* **18** 055006
[29] Reichardt B, Unger F and Vazirani U 2013 A classical leash for a quantum system: command of quantum systems via rigidity of CHSH games *Nature* **496** 456–60
[30] Rosicka M, Ramanathan R, Gnaci?ski P, Horodecki K, Horodecki M, Horodecki P and Severini S 2016 Linear game non-contextuality and bell inequalities?a graph-theoretic approach *New J. Phys.* **18** 045020
[31] Schwarz S, Bessire B, Stefanov A and Liang Y-C 2016 Bipartite bell inequalities with three ternary-outcome measurements–from theory to experiments *New J. Phys.* **18** 035001
[32] Shor P W 1997 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM J. Comput.* **26** 1484–509
[33] Summers S J and Werner R 1987 Bell's inequalities and quantum field theory. i. general setting *J. Math. Phys.* **28** 2440
[34] Supic I, Augusiak R, Salavrakos A and Ac?n A 2016 Self-testing protocols based on the chained bell inequalities *New J. Phys.* **18** 035013
[35] Supic I and Hoban M J 2016 Self-testing through epr-steering *New J. Phys.* **18** 075006
[36] Tamaki K, Curty M and Lucamarini M 2016 Decoy-state quantum key distribution with a leaky source *New J. Phys.* **18** 065008
[37] Thinh L P, de la Torre G, Bancal J-D, Pironio S and Scarani V 2016 Randomness in post-selected events *New J. Phys.* **18** 035007
[38] Vazirani U and Vidick T 2014 Fully device-independent quantum key distribution *prl* **113** 140501
[39] Wang Y, Wu X and Scarani V 2016 All the self-testings of the singlet for two binary measurements *New J. Phys.* **18** 025021
[40] Woodhead E 2016 Semi device independence of the bb84 protocol *New J. Phys.* **18** 055010